A silent digital witness

Other

A silent digital witness

The ethos that "every contact leaves a trace" is as true in the digital environment as in a conventional crime scene. Ian Kennedy explains

WHEN DR HAROLD SHIPMAN was in his surgery fabricating the medical records of his victims, he was unaware that the very computer he was using was silently auditing every false date he entered onto the medical records. Ironically, the very tool he was using to commit this attempt at deception would later become a witness against him. Dr Shipman's surgery computer had become its very own digital crime scene.

Digital crime scene

Digital devices such as computers hold a wealth of information about recent and in some cases much less recent activities. Many actions performed by a user are surreptitiously recorded and stored away in various locations, as Shipman found out to his cost.

This audit trail of user activity takes place for a number of reasons. For example, audit trails are created to assist the user in the recall of actions at a later date such as the recall of internet history or recently opened documents.

Also, the normal behaviour of the Windows operating system will commonly create data relating to user activity in system files such as those created by the system restore process, a file backup system.

The Windows operating system is also notoriously untidy at creating temporary files and subsequently failing to delete them.

For Shipman, it was the fact that he clearly falsified his records. For paedophiles, the keywords typed into search engines such as Google, details of the files downloaded and opened are all recoverable.

Actions such as these are indicative of the user's intent to search for subject matter on the internet, download and afterwards view the contents. Consequently, a plethora of evidence awaits a forensic examiner to demonstrate not simply the *mens rea* but also the *actus reus* of an alleged crime.

Digital DNA

Unlike a conventional crime scene, the very existence of evidence may not be obvious to the first person on the scene, called the first responder. There are no easily identifiable items of evidence, such as footprints or bloodstains for them to identify and preserve.

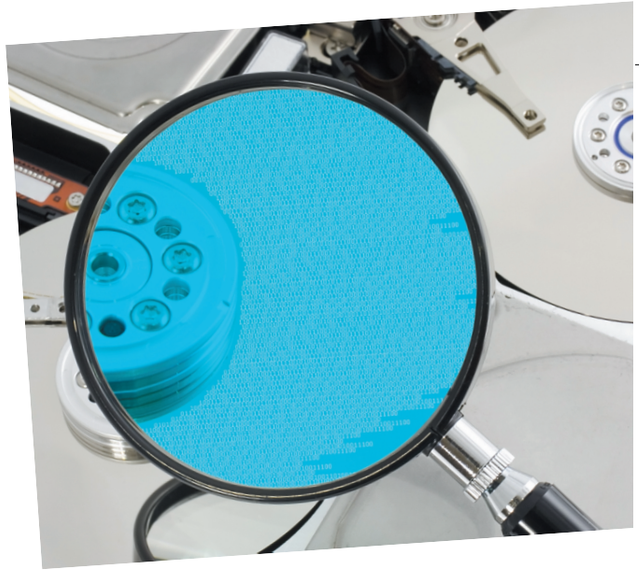
Conventional forensics follows the ethos of Locard's exchange principle: namely that "Every contact leaves a trace". Similar to evidence such as DNA, digital evidence is fragile. Every click of the mouse could potentially alter the data on the device and thus destroy vital evidence. Thus, if a device such as a computer is already in a powered on state at the arrival of a first responder they must not 'have a look around' on the computer prior to powering the device down as this threatens the integrity of the evidence contained on the computer.

Following best practice

Given the fragility of digital evidence, good practice and competence is vital. The Association of Chief Police Officers (ACPO) of England, Wales and Northern Ireland recently updated its *Good Practice Guide for Computer-Based Electronic Evidence*. In this document (aimed at first responders, forensic analysts and managers alike) are identified four guiding principles. These principles influence many of the procedures followed when seizing and examining a digital device are:

- Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
- Principle 2: In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The training and experience of the analyst undertaking the work has always bore witness to their competence. More recently, the Council for the Registration of Forensic Practitioners has formed a digital forensics specialty to provide a peer review system for analysts.



Blinded by the science

The bewildering array of terminology associated with computers is sometimes used in an attempt to mislead. Anyone involved in digital forensics must familiarise themselves with terms such as sectors, clusters, live and deleted files, slack space and timestamps.

On a computer, data is typically stored on a device called a hard disk. Data is stored in one or more equally sized areas called sectors. This is similar to your average high street that contains a mixture of small businesses occupying a single address on the street and the larger businesses that occupy several addresses on the street. Files that are too big to fit into a single sector will overflow into further sectors.

Because there are so many sectors to address on a computer, they are read from and written to typically in multiples of four sectors at a time. These grouped sectors are called clusters. Clusters that are associated with a file are known as allocated clusters, while those that are no longer associated (see deleted files below) or have not yet been associated with a file are known as unallocated clusters.

Live and deleted files

Evidence residing in files that are clearly visible to the user and can be readily viewed with a suitable computer program are typically known as 'live' files. The average computer user will work almost exclusively with live files. But finding evidence on a digital device such as a computer is not always as straight forward as looking at the live files located on a hard disk. It is common for data that is evidentially significant to be located in areas that are far less familiar to the average computer user.

Files moved to the recycle bin are not deleted from the computer immediately. Under normal circumstances, when the user deletes a file on a modern Windows computer, the file is initially moved to a special folder called the recycle bin. If the user then empties the recycle bin the sectors that were allocated to that file are freed up for use by any new or existing files.

This means when the user clicks on the recycle bin folder to view its contents the file will appear to have disappeared from the list of files contained within it.

Although the file no longer appears in the folder, it is not actually deleted. It remains on the disk until it is overwritten by another file. An analogy of this situation is when you decide you no longer want to keep that two-hour movie on your VHS tape you recorded. You cross out the title on the spine label but do not erase the tape.

Instead you put it to one side for reuse another time. In the case of the file on the hard disk, it too remains untouched on the disk. Thus, any data found in this area at one time belonged to a file, which has since been deleted but now resides in the unallocated clusters of the disk.

When new data being written to a hard disk does not completely overwrite the old data within a cluster (remember, the computer reads and writes to the hard disk in multiples of four sectors) then the data that has not been overwritten is said to reside in the slack space of a file.

Returning to our VHS analogy, imagine you take that tape with the two-hour movie on it and then recorded over it from the beginning again with a 30-minute programme. The 90 minutes of footage following the new programme is data from the 'slack space'.

Typically, one of the key elements to an indictment is the date and time of the offence. Digital evidence such as files that are exhibited will be produced with a number of associated dates and times (collectively known as timestamps). The basic timestamps are:

- **Date created**
  The timestamp of when the file first existed on the current hard disk. Usually, this is the true date and time the file was indeed created, but if the file is copied to a new hard disk, then the date created value will change to the timestamp of this event.
- **Date last modified**
  The timestamp of when data was last written to the file.
- **Date last accessed**
  Not simply the timestamp of when the file was last read by the user, but also the date and time it was accessed by the Windows operating system or a program such as an anti-virus application.

State of the digital art

One of the most exciting areas of research in the world of digital forensics is the analysis of live data, also known as live forensics.

Conventional forensics is a 'post-mortem' process whereby the data contained on a digital device such as a hard disk is examined after the power has been removed. Live forensics is concerned with the acquisition and examination of data contained in the volatile memory of a device that is in a powered on state. Once power is removed, such data is lost.

'Clusters are read from and written to typically in multiples of four sectors at a time'

Data such as recently entered passwords, documents written but not saved or even encrypted files that are open in an unencrypted state are examples of the kind of data that could be retrieved from the volatile memory (also known as random access memory or RAM).

To extract a copy of the memory on a live device such as a computer typically involves making changes to the data in the device's memory so it is therefore necessary to ensure that principle 2 of the ACPO guidelines is adhered to.

This makes the competence of the analyst and principle 3, the generation of a detailed audit trail, even more important.

In recognition of this newly emerging area of digital forensics, the recently updated ACPO guidelines has a new section specifically dealing with the seizure of live evidence.

When live data is analysed and captured on a suspect computer the impact and behaviour of any commands and programs executed must be known and thoroughly understood by the forensic computer analyst.

Therefore, only trusted specialised tools should be used to conduct the procedures. All actions performed should, of course, be documented to comply with principle 3.

Conclusions

Many of the actions you perform on a computer are silently recorded. Evidentially, this data can show the actions and the intentions of the suspect. Like DNA, it is also fragile and so competence and procedure are vital. The use of live forensics is a growing field of investigation and although still in its infancy, has now become part of the nationally accepted best practice.

◆ Ian Kennedy is a forensic computer analyst at the Digital Forensics Unit of Kent police